Procedure NO: 2205.08 Intrusion Detection Systems and Firewall Procedures
Reference: Policy No: 2205
Effective: 12/28/04
Prior Issue: N/A

Purpose:

MIS employees per Government Information Technology Agency (GITA) P800-S830 shall maintain all Security related network equipment.

Rules

1. **MIS PERSONNEL** will be proactive in finding ways to be alerted to Security Bulletins or technical information regarding best security practices.

2. **MIS** shall create systems to log and monitor network activity for reporting purposes.

3. **MIS** shall ensure that all public access is conducted on the Demilitarized Zone (DMZ) network.

4. **MIS** shall ensure all network devices (Local Area Network (LAN)/Wide Area Network (WAN) systems switches/routers) are appropriately updated and controlled.

5. **MIS** shall ensure that the Intrusion Detection System (IDS) signatures are updated on a monthly basis.
   a. **MIS** shall report all IDS logged intrusions successful or not to State Information Protection Center (SIPC).
      i. MIS shall be notified on all IDS signature attempts through automatic notifications.

6. **MIS** shall ensure that:
   a. An incoming packet shall not have a source address of the internal network;
   b. An incoming packet shall have an outside registered destination address associated with the internal network, if static or dynamic NAT is employed;
   c. An outgoing packet shall have a source address of the internal network.;
   d. An outgoing packet shall not have a destination address of the internal network;
   e. An incoming or outgoing packet shall not have a source or destination address that is private or listed in RFC 1918 reserved space,
   f. Any source routed packets or any packets with the IP options field set shall be blocked, and
   g. Reserved, DHCP auto-configuration and multicast addresses should be blocked.
   h. Firewall technologies should be managed via encrypted communications.

7. **MIS** shall ensure that unused services should be turned off, unused ports disabled, and logging capability turned on any device that is capable of logging.

8. **MIS** shall approve hardware, operating systems, services and applications as part of the pre-deployment review phase.

9. **MIS** shall ensure that operating system configuration be done according to the secure host and router installation and configuration standards

10. **MIS** shall disable services and applications not serving business requirements.

11. **MIS** shall approve and document trust relationships between systems may only be introduced according to business requirements.

12. **MIS** shall ensure services and applications not for general access be restricted by access control lists and firewalls.

13. **MIS** shall ensure insecure services or protocols be replaced with more secure equivalents whenever such exist.

14. **MIS** shall ensure any remote administration be performed over secure channels (e.g., encrypted network connections using SSH or IPSEC) or console access independent from the DMZ networks. Where a methodology for secure channel connections is not available, one-time passwords (DES/SofToken) shall be used for all access levels.

15. **MIS** shall ensure all host content updates shall occur over secure channels.

16. **MIS** shall log security-related events and audit trails which are saved to MIS approved logs. Security-related events include (but are not limited to) the following:
    a. User login failures;
    b. Failure to obtain privileged access;
    c. Access policy violations.

17. **MIS** shall address non-compliance waiver requests on a case-by-case basis and approve waivers if justified.
    a. All communication from servers on the DMZ to internal applications and services shall be controlled;
    b. Remote or dial-in access to networks shall be authenticated at the Agency firewall, or through services placed on the Agency DMZ;
    c. There shall be no public access to the internal network without authentication. The DMZ is the appropriate location for web servers, external DNS servers, VPN, and dial-in servers;
    d. All remote access users should be considered external and subjected to the firewall rule set. VPNs should terminate on the external segment or outside of the firewall.

18. **MIS** shall report any of the following acts by any person or network address who, without authority or acting in excess of authority to SIPC:
    a. Accesses an IT device (server, storage, or client) or network with the intent to instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of a computer, computer system, or network;
    b. Accesses, alters, damages, or destroys any IT device, network, or any physically or logically connected IT devices;
    c. Accesses, alters, damages, or destroys any computer application systems, programs, or data;
    d. Recklessly disrupts or causes the disruption of any services provided through the use of any IT device or network;
    e. Denies or causes the denial of IT-related services to any authorized user of those services;
    f. Recklessly uses an IT device or network to engage in a scheme or course of conduct that is directed toward another person and that seriously alarms, torments, threatens, or terrorizes the person;
    g. Prevents a computer user from exiting an Internet, Intranet, or internal host site, computer system, or network-connected location in order to compel the user's computer to continue communicating with, connecting to, or displaying the content of the service, site, or system;
    h. Knowingly obtains any information that is required by law to be kept confidential or any records that are not classified as public records by accessing an IT device or network that is operated by the State, a political subdivision of the State, or a medical institution;
    i. Introduces a computer-related contaminant (e.g., malicious code, virus, worm, etc.) into any IT device or network;

j. Makes multiple attempts to access an IT device or network system within a brief period of time.

19. **MIS** shall ensure that intrusion detection mechanisms for servers shall include the use of software and review procedures that scan for unauthorized changes to files, including system files.

20. **MIS** shall ensure Software and review procedures shall examine network traffic for known, suspicious attack signatures or activities and look for network traffic indicative of devices that have been misconfigured.

21. Violations of set IDS parameters shall trigger appropriate notification to security administrators or agency personnel, allowing a response to be undertaken. **MIS** shall report IDS intrusions and attempts to the State Information Protection Center (SIPC) within one hour of being notified.

a. The following information, at a minimum, is required when reporting intrusions to SIPC:

i. Agency name;

ii. The Agency SIPC Coordinator's name and phone number; and

iii. Brief description of intrusion and damages (real or anticipated).

b. Whenever possible, **MIS** will capture and maintain log entries for a minimum of one week following the detection of intrusion (or longer at the discretion of the application or system owner). Log entries provide significant detail that can be used for investigation and prosecution of the intruder, Form 2205.03A.

Effective Date:	**Approved by Process Owner:**	**Review Date:**	**Reviewed By:**